Unconditional Security Proof of Decoy-State Quantum Key Distribution with Arbitrary Intensity Error Pattern of Light Pulses

Xiang-Bin Wang,[1] Cheng-Zhi Peng,[1,2] Jun Zhang,[2] and Jian-Wei Pan[1,2,3]

[1]*Department of Physics, Tsinghua University, Beijing 100084, China*

[2]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany*

Abstract

We show the unconditional security of decoy-state method with whatever intensity error pattern if the intensity upper bound of decoy pulses and intensity lower bound of signal pulses are known. Our result immediately applies to the existing experimental data.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

Introduction.— Quantum key distribution (QKD) [1, 2, 3] is a type of very important quantum algorithm that can be used for secure private communication between two remote parties, Alice and Bob. However, the standard QKD protocols such as the so called BB84 protocol [1] requests a perfect single-photon source which is a difficult technique. Most of the existing set-ups realize the standard BB84 protocol through using weak coherent light as the approximate probabilistic single-photon source. Such an implementation in principle suffers from the photon-number-splitting attack [4, 5]. The decoy-state method [6, 7, 8, 9, 10] and some other methods [11, 12, 13] can be used for unconditionally secure QKD even Alice only uses an imperfect source, e.g., a coherent light [4, 5]. According to the separate theoretical results of ILM-GLLP [14], if one knows the upper bound of the fraction of tagged bits (those raw bits generated by multi-photon pulses from Alice) or equivalently, the lower bound of the fraction of un-tagged bits (those raw bits generated by single-photon pulses from Alice), a secure final key can be distilled even though an imperfect source is used in the protocol. The goal of decoy-state method is to verify such bounds faithfully and efficiently. Recently, a number of experiments on decoy-state QKD have been done [15, 16, 17]. However, the existing theory of decoy-state method assumes the exact control of pulse intensities. In this Letter, we study this problem and we present a theorem that immediately applies to all existing experimental results.

Foundations of decoy-state method QKD.— We shall summarize the existing theory of decoy-state method [6, 7, 8, 9] starting from the definition of the *counting rate*. Given a class of N pulses, after Alice sends them out to Bob one by one, if Bob observes n counts at his side, the counting rate for pulses in this class is

$$s = n/N. \tag{1}$$

In some other literatures, the term of *yield* is used.

Proposition 1: If class X is divided into l subclasses and any pulse in X belongs to only one subclass, then the total number of counts at Bob's side due to pulses in class X must be equal to the summation of numbers of counts due to the pulses of each subclasses.

If the fractions of pulses in each subclasses are $a_0, a_1 \cdots, a_l$, proposition 1 is equivalent to the following formula in counting rates of each subclass.

$$S_X = \sum_0^l a_i s_i \tag{2}$$

where S_X is the counting rate of class X, s_i is the counting rate of the ith subclass.

Proposition 2. If pulses in class X are independent and identical, the counting rates of any two random subclasses of pulses from class X must be equal to each other given whatever channel, if the number of pulses in each subclass is sufficiently large.

Proposition 3. If we have two classes X and X'. Suppose y is a subclass of X and y' is a subclass of X'. Pulses of these two subclass are independent and in the same state. If y and y' are randomly mixed and then sent to Bob, the counting rate of subclass y and the counting rate of subclass y' must be equal, *even though the state of pulses of class X is different from that of class X'.*

This is a direct consequence of proposition 2. Here pulses of subclasses y, y' can be regarded as one class, $y \cup y'$. The state for pulses of y is identical with that from y', all pulses in class $y \cup y'$ are actually independent and identical. Therefore y can be regarded as one *random* subclass of class $y \cup y'$ therefore Proposition 2 applies. Proposition 3 is the heart of the decoy-state idea.

A coherent state of intensity x is

$$\rho_x = \sum_{n=0}^{\infty} \frac{x^n e^{-x}}{n!} |n\rangle\langle n|. \tag{3}$$

In the decoy-state protocol, Alice may choose $x = 0, \mu, \mu'$ $(1 \geq \mu' > \mu)$ randomly at each time, with probabilities p_0, p, p' for each intensity and $p_0 + p + p' = 1$. Pulses of these 3 different intensities can be regarded as 3 classes (sources), Y_0, Y, Y'. In particular, for $x = \mu$, the state can be written in the convex form of

$$\rho_\mu = a_0|0\rangle\langle 0| + a_1|1\rangle\langle 1| + a_c\rho_c \tag{4}$$

with $a_0 = e^{-\mu}, a_1 = \mu e^{-\mu}, a_c = 1 - e^{-\mu} - \mu e^{-\mu}$ and $a_c\rho_c = \rho_\mu - a_0\rho_0 - a_1\rho_1 = \sum_{n=2}^{\infty} \frac{e^{-x}x^n}{n!}|n\rangle\langle n|$. For simplicity, we shall call pulses from this class as *decoy pulses*. In producing such a state, Alice *could* have actually used three sub-sources y_0, y_1, y_c with probability a_0, a_1, a_c. These three sub-sources produce states $|0\rangle\langle 0|, |1\rangle\langle 1|$ and ρ_c, respectively. We can regard pulses from each sub-source as a subclass, i.e., pulses from sub-sources y_0, y_1, y_c are regarded as subclasses y_0, y_1, y_c of class Y (the decoy pulses). According to Proposition 1 or Eq.(2),

$$S_\mu = a_0 s_0 + a_1 s_1 + a_c s_c. \tag{5}$$

Here S_μ, s_0, s_1, s_c are the counting rates of all decoy pulses (i.e. all pulses in class Y), subclass y_0, subclass y_1, and subclass y_c, respectively.

For intensity $x = \mu'$, the coherent state ρ_x is

$$\rho_{\mu'} = a'_0|0\rangle\langle 0| + a'_1|1\rangle\langle 1| + a'_c\rho_c + a'_d\rho_d \tag{6}$$

with $a'_0 = e^{-\mu'}, a'_1 = \mu' e^{-\mu'}, a'_c = \frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}} a_c$ and $a'_d > 0$, ρ_d is a density operator. For simplicity, we shall call pulses of this intensity as *signal pulses*. In producing a signal pulse, Alice *could* have actually used another four sub-sources y'_0, y'_1, y'_c, y'_d with probability a'_0, a'_1, a'_c, a'_d whenever she decides to send a signal pulse. These four sub-sources produce states $|0\rangle\langle 0|, |1\rangle\langle 1|, \rho_c$ and ρ_d, respectively. According to Proposition 1,

$$S_{\mu'} = a'_0 s'_0 + a'_1 s'_1 + a'_c s'_c + a'_d s'_d \tag{7}$$

and $S_{\mu'}, s'_0, s'_1, s'_c, s'_d$ are the counting rate of all signal pulses (i.e., all pulses in class Y'), subclass y'_0, subclass y'_1, subclass y'_c and subclass y'_d respectively. In the protocol, Alice decides to use intensity $0, \mu, \mu'$ randomly, therefore the pulses of all subclasses are randomly mixed. According to Proposition 3,

$$s_0 = s'_0 = S_0, \;\; s_1 = s'_1, \;\; s_c = s'_c \tag{8}$$

where S_0 is the counting rate of class Y_0. Eq. (5,7) is equivalent to

$$\begin{cases} \mathcal{S} = a_1 s_1 + a_c s_c \\ \mathcal{S}' = a'_1 s_1 + a'_c s_c \end{cases} \tag{9}$$

and $\mathcal{S} = S_\mu - a_0 S_0$; $\mathcal{S}' = S_{\mu'} - a'_0 S_0 - a'_d s'_d$. Therefore,

$$s_1 = \frac{a'_c \mathcal{S} - a'_1 \mathcal{S}'}{a'_c a_1 - a'_1 a_c}. \tag{10}$$

Since Alice herself decides which time to use which intensity in the protocol, she knows which pulse belongs to which class (Y_0, Y, Y'). After Bob announces those specific time windows when his detector has counted, Alice can calculate $S_0, S_\mu, S_{\mu'}$ by Eq.(1). Therefore $S_0, S_\mu, S_{\mu'}$ are *known* parameters in the protocol. In the case that the pulse intensity is exactly controlled, actually only the parameter s'_d is unknown. Therefore, it will be secure if we find the smallest value s_1 satisfying the equation above among all possible values for parameters $\mathcal{S}'$. Obviously, the largest value $\mathcal{S}'$ produces the smallest value s_1. So we only need to set $a'_d s'_d = 0$. This is equivalent to the prior art result [7].

The unconditional security for decoy-state QKD with whatever pattern of intensity error.—

In the above results of 3-intensity protocol with coherent states, the *independent* pulses are assumed for each class therefore classical sampling theory works directly. In practice, as a continuous variable, the intensity cannot be controlled exactly. There can be intensity errors to each pulses in class Y (decoy pulses) and class Y' (signal pulses). Most generally, the actual intensity of decoy pulses produced at different times are $\{\mu_i\}$, i is from 1 to N, the total number of decoy pulses; the actual intensity of signal pulses produced at different times are $\{\mu'_i\}$, i is from 1 to N', the total number of signal pulses. The intensity errors of different pulses can be *correlated*. For example, the intensity can be dependent on the temperature. In a certain interval, all pulses can be brighter or darker than the supposed value. Due to this possible correlation, neither the decoy pulses nor the signal pulses are *independent*, the state of decoy pulses or signal pulses cannot be simply represented by a *single-pulse* density operator. This makes it unclear on how to apply the classical sampling theory. Consider an extreme example, the actual intensity of each pulse is 10% larger than the supposed one in the first half of quantum-state transmission, 10% lower than the supposed one in the second half of the transmission. If Eve's channel transmittance is 4η during the first half of pulse transmission and η during the second half of pulse transmission, overall counting rates for single-photon pulses from subclass y_1 (all those single-photon pulses from class Y) is larger than that of subclass y'_1 (all those single-photon pulses from class Y'). The ratio of these two values is 1.023 if the supposed intensity for decoy pulses and signal pulses are $0.2, 0.6$, respectively. This conflicts with Proposition 3 because here y_1 and y'_1 are *not* randomly mixed: the ratio of occurring probability of y_1 to the occurring probability of y'_1 throughout the protocol is *not* constant at different time intervals.

To overcome this problem, our main idea is this: we can choose a subclass $\tilde{y}'_1 \subseteq y'_1$ and a subclass $\tilde{y}'_c \subseteq y'_c$ so that the occurring probabilities of a pulse from $\tilde{y}'_1$ and a pulse from $\tilde{y}'_c$ are constant throughout the protocol. We can then use the existing decoy-state theory to pulses of three classes of Y_0, Y and $\tilde{Y}' = \tilde{y}'_1 \cup \tilde{y}'_c \subseteq Y'$.

Consider a virtual protocol, *Protocol 1:* At each time i in sending a pulse to Bob, Alice produces a two-pulse (pulse A and pulse B) bipartite state

$$\rho_i(2) = p_0|z_0\rangle\langle z_0| \otimes |0\rangle\langle 0| + p|z_1\rangle\langle z_1| \otimes \rho_\mu + p'|z_2\rangle\langle z_2| \otimes \rho_{\mu'_i}. \tag{11}$$

Here the first subspace is for pulse A and the second subspace is for pulse B. Alice keeps pulse A and sends out pulse B to Bob. The value μ keeps to be constant but μ'_i can change

from time to time and any μ_i' is not less than the constant value μ', with i from 1 to N_t, the total number of pulses sent out. States $\{|z_x\rangle\}$ are orthogonal to each other for different x ($x = 0, 1, 2$) and $p_0 + p + p' = 1$. Later, Alice measures A pulse in ($\{|z_x\rangle\}$) basis and she can know which B pulse belongs to which class (Y_0, Y or Y'). State ρ_μ can be written in the convex form of Eq.(4). The state $\rho_{\mu_i'}$ is

$$\rho_{\mu_i'} = \sum_{n=1}^{\infty} \frac{e^{-\mu'}\mu'^n}{n!}|n\rangle\langle n| + e^{-\mu'}|0\rangle\langle 0| + \sum_{n=1}^{\infty}\left(\frac{e^{-\mu_i'}\mu_i'^n}{n!} - \frac{e^{-\mu'}\mu'^n}{n!}\right)|n\rangle\langle n| \tag{12}$$

Since $\mu_i' \geq \mu'$, $\frac{e^{-\mu_i'}\mu_i'^n}{n!} - \frac{e^{-\mu'}\mu'^n}{n!} \geq 0$ for all n provided that μ_i' is not too large, e.g., $\mu_i' \leq 1$. Furthermore, the following convex form holds since $\mu' > \mu$:

$$\sum_{n=1}^{\infty} \frac{e^{-\mu'}\mu'^n}{n!}|n\rangle\langle n| = e^{-\mu'}\mu'|1\rangle 1| + \frac{\mu'^2 e^{-\mu'} a_c}{\mu^2 e^{-\mu}}\rho_c + \sum_{n=3}^{\infty}\left(\frac{e^{-\mu'}\mu'^n}{n!} - \frac{e^{-\mu}\mu^n}{n!}\right)|n\rangle\langle n| \tag{13}$$

and a_c is define in Eq.(4). Therefore

$$\rho_{\mu_i'} = a_1'|1\rangle\langle 1| + a_c'\rho_c + (1 - a_1' - a_c')\rho_e^i, \tag{14}$$

where $a_1' = \mu' e^{-\mu'}$, $a_c' = \frac{a_c \mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}}$ are constant for whatever i. We don't need the explicit formula for ρ_e^i. To anybody outside Alice's lab, Alice *could* have used a three-pulse (pulse A, A', B) tripartite state of

$$\begin{aligned}\rho_i(3) = {} & p_0|z_0\rangle\langle z_0| \otimes |z_0\rangle\langle z_0| \otimes |0\rangle\langle 0| \\ & + p|z_1\rangle\langle z_1| \otimes (a_0|v_0\rangle\langle v_0| \otimes |0\rangle\langle 0| + a_1|v_1\rangle\langle v_1| \otimes |1\rangle\langle 1| + a_c|v_c\rangle\langle v_c| \otimes \rho_c) \\ & + p'|z_2\rangle\langle z_2| \otimes \left[a_1'|v_1'\rangle\langle v_1'| \otimes |1\rangle\langle 1| + a_c'|v_c'\rangle\langle v_c'| \otimes \rho_c' + (1 - a_1' - a_c')|v_e'\rangle\langle v_e'| \otimes \rho_e^i\right]\end{aligned} \tag{15}$$

and $\{\{|v_x\rangle|x = 0, 1, c\}, \{|v_x'\rangle|x = 0, 1, e\}\}$ are all orthogonal to each other. Alice keeps A pulses and A' pulses (those pulses in the first and second subspace) and sends out B pulses (the pulses in the third subspace) to Bob. Given this, we can define the following subclasses: if Alice obtains her measurement outcome of $|v_0\rangle, |v_1\rangle$ or $|v_c\rangle$ after measuring the A' pulse, the corresponding pulse sent out (B pulse) is regarded as a pulse of subclass y_0, y_1 or y_c, and here $y_0 \cup y_1 \cup y_c = Y$; if Alice obtains her measurement outcome of $|v_1'\rangle, |v_c'\rangle$ or $|v_e'\rangle$ after

measuring her A' pulse, the corresponding pulse sent out is regarded as a pulse of subclasses $\tilde{y}'_1, \tilde{y}'_c$ or $\tilde{y}'_e$ and here $\tilde{y}'_1 \cup \tilde{y}'_c \cup \tilde{y}'_e = Y'$. Given such definitions, the occuring probability of a pulse from $\tilde{y}'_1, \tilde{y}'_c$ is *constant*. Therefore we can use Proposition 1 and Proposition 3 for class Y and class $\tilde{Y}' = \tilde{y}'_1 \cup \tilde{y}'_c$:

$$\begin{cases} a_1 s_1 + a_c s_c = \mathcal{S} \\ a'_1 s_1 + a'_c s_c = \tilde{\mathcal{S}}' \end{cases} \tag{16}$$

with $\tilde{\mathcal{S}}'$ being the counting rate of pulses in class $\tilde{Y}'$, $\mathcal{S} = S_\mu - e^{-\mu} s_0$, s_1 is the counting rate of class y_1 or $\tilde{y}'_1$, s_c is the counting rate of class y_c or $\tilde{y}'_c$. In non-asymptotic case, the counting rates of subclass $\tilde{y}'_1$ and subclass $\tilde{y}'_c$ are $s'_1 = (1 - r_1)s_1$, $s'_c = (1 - r_c)s_c$ and $s_0 = (1 + r_0)S_0$. Eq.(16) is replaced by

$$\begin{cases} a_1 s_1 + a_c s_c = \mathcal{S} \\ (1 - r_1) a'_1 s_1 + (1 - r_c) a'_c s_c = \tilde{\mathcal{S}}' \end{cases} \tag{17}$$

The range of r_0, r_1, r_c can be set to be

$$|r_x| \leq 10 \sqrt{\frac{1}{a_x N s_x}}, \ |r_0| \leq 10 \sqrt{\frac{1}{S_0 N_0}} \tag{18}$$

with $x = 1, c$; N, N_0 being the number of decoy pulses and number of pulses in Y_0. The possibility that the actual value of r_x goes beyond the above ranges is exponentially close to 0 [7]. The number of counts caused by a subclass cannot be larger than that of a whole class and $\tilde{Y}'$ is a subclass of Y'. Therefore $N'(a'_1 s_1 + a'_c s_c) \leq N' S_{\mu'}$, i.e., $\mathcal{S}' \leq S_{\mu'}$. We can then solve Eq.(17) numerically over all possible values of

$$0 \leq \tilde{\mathcal{S}}' \leq S_{\mu'} \tag{19}$$

and pick out the smallest value of s_1. Doing it in this way, Alice actually does not need any information of which pulse belong to which subclass (She only needs the information of which pulse belongs to which class, Y_0, Y, Y'). Therefore she can discard pulse A' of the tripartite state $\rho_i(3)$. This means, she can simply use the bipartite state $\rho_i(2)$ and obtain s_1 value through Eq.(17). Thus the lower bound of single-photon transmittance is verified. This can be summarized as

Lamma 0: *Protocol 1* is secure provided that $\mu'_i \geq \mu'$ and Eq.(17) is used for the lower bound of single-photon counts.

Lemma 1: Alice can use Eq.(17) safely if she uses any source that in principle can be produced through attenuating B pulse of state $\rho_i(2)$.

Proof: Suppose in another protocol, *Protocol 2*, at any time i, Alice's source generates a bipartite state γ_i which can in principle be obtained through attenuating pulse B of $\rho_i(2)$ by a factor χ_i. If Eve can attack *Protocol 2* effectively by scheme $\mathcal{A}$ then Eve can also attack *Protocol 1* effectively by first attenuating the pulses by a time-dependent factor χ_i and then using scheme $\mathcal{A}$. This completes the proof.

Lemma 2: Alice can safely use Eq.(17) if she actually at each time had used any state $W_i = p_0|z_0\rangle\langle z_0| \otimes |0\rangle 0| + p|z_1\rangle\langle z_1| \otimes \rho_{\nu_i} + p'|z_2\rangle\langle z_2| \otimes \rho_{\nu_i'}$ provided that $\nu_i \leq \mu$ and $\nu_i' \geq \mu'$. (Here $\rho_{\nu_i}, \rho_{\nu_i'}$ are coherent states of intensity ν_i, ν_i').

Proof: Denote the (time-dependent) attenuation factor $\omega_i = \frac{\nu_i}{\mu}$. Construct a specific setting of *Protocol 1* with $\mu_i' = \frac{\nu_i'\mu}{\nu_i}$ and constant value μ for the bipartite state $\rho_i(2)$ there. According to Lemma 0, *Protocol 1* with such a specific setting is secure since $\frac{\nu_i'\mu}{\nu_i} \geq \nu_i' \geq \mu'$. After attenuating B pulse in each $\rho_i(2)$ by the factor ω_i, $\rho_i(2)$ is changed to state W_i. According to our lemma 1, Alice can use W_i directly and then use Eq.(17) for lower bound of s_1. Moreover, it is of no difference if Alice measures each A pulse in basis $\{|z_x\rangle\}$ in the very beginning. If she does this, the protocol with source state W_i is changed into a 3-intensity protocol with intensities $0, \{\nu_i\}, \{\nu_i'\}$ and $\nu_i \leq \mu$, $\nu_i' \geq \mu'$, with probability p_0, p, p' for using each of them at each time. Consequently we arrive at the following theorem:

Theorem: The 3-intensity protocol is secure with whatever intensity error pattern of decoy pulses (class Y) and signal pulses (class Y') provided that:

1) the intensity of each decoy pulses is not larger than μ and the intensity of each signal pulses is not less than μ' (but not larger than 1);

2) Eq.(17) is used to calculate the lower bound of s_1 in the range of $0 \leq \tilde{\mathcal{S}}' \leq S_{\mu'}$.

Our theorem here applies to all existing experiments immediately if the intensity upper bound of decoy pulses and lower bound of signal pulses are known. In one of the recent experiment [16], the intensities for decoy pulse and signal pulse are set around 0.2 and 0.6 respectively. There could be up to $\pm 5\%$ fluctuation to each pulse. We can safely assume that the intensity of decoy pulses is not larger than $\mu = 0.21$ and the intensity of signal pulses is not smaller than $\mu' = 0.57$. We use the data for QKD distance of 50 km [19]. After s_1, s_1' is calculated based on our theorem, the final key rate is calculated in the same way used in Ref. [16]. The key rate decreases drastically with the increase of intensity fluctuation, as

TABLE I: Unconditionally secure key rate (R) vs different values of intensities error upper bound (δ_M) using the experimental data in the case of 50 km [16]. The experiment lasts for 1481.2 seconds with the repetition rate 4 MHz. The three counting rates are $S_{\mu'} = 3.817 \times 10^{-4}, S_{\mu} = 1.548 \times 10^{-4}, S_0 = 2.609 \times 10^{-5}$ and the observed quantum bit error rates (QBER) for signal states and decoy states are $4.247\%, 8.379\%$ respectively.

δ_M	5%	4%	3%	2%	1%	0
$s_1'/10^{-4}$	5.090	5.284	5.472	5.654	5.831	6.004
R (Hz)	30.408	43.008	55.357	67.476	79.381	91.089

shown in Table I. The intensity fluctuation can be controlled less than 1% in the experiment done by Yuan et al [18].

Acknowledgemet: This work is supported by National Fundamental Research Program of China, NNSF China, and Tsinghua Bai Ren program.

[1] C.H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984)*, pp. 175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] M. Dusek, N. Lütkenhaus, M. Hendrych, in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, 2006).

[4] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H.P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[5] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[7] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[8] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[9] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[10] J.W. Harrington *et al.*, quant-ph/0503002.

[11] R. Ursin *et al.*, quant-ph/0607182.

[12] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A 72, 032301 (2005).

[13] M. Koashi, Phys. Rev. Lett., 93, 120501(2004); K. Tamaki, N. Lükenhaus, M. Loashi, J. Batuwantudawe, quant-ph/0608082

[14] H. Inamori, N. Lütkenhaus, D. Mayers, quant-ph/0107017; D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[15] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, quant-ph/0601168.

[16] Cheng-Zhi Peng, Jun Zhang, Dong Yang, Wei-Bo Gao, Huai-Xin Ma, Hao Yin, He-Ping Zeng, Tao Yang, Xiang-Bin Wang and Jian-Wei Pan, quant-ph/0607129; to appear in Phys. Rev. Lett.

[17] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita and S. W. Nam, quant-ph/0607186; to appear in Phys. Rev. Lett.

[18] Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, quant-ph/0610015.

[19] This part of data is not completely listed in Ref [16].